Avoiding Phishing Attacks in Online Voting System

Keerthika J[1*], Rasha R[2], Rasi L[3], Riya Sherin C[4] & Snekha Lakshmi N.B.[5]

[1-5]*Department of Computer Science and Engineering, Sri Eshwar College of Engineering and Technology, Coimbatore, India.*
*Corresponding author email: keerthika.janarthanan@gmail.com**

DOI: http://doi.org/10.46431/MEJAST.2022.5206

Article Received: 22 February 2022 *Article Accepted: 27 April 2022* *Article Published: 31 May 2022*

ABSTRACT

This work's main purpose is to provide a secure voting system that fits all of the voting process' requirements, including authentication, confidentiality, and morality. Simplicity is also required to guarantee that ordinary people participate. Other factors to consider are dependability, convenience, flexibility, mobility, and affordability, in addition to security and simplicity. We wanted to build a system where the whole encryption and decryption of the ballots is transparent and nevertheless safe to ensure that the user utilizes a secure voting system.

Keywords: *Cryptography, Security, Authentication, Online voting.*

1. Introduction

Voting is a basic right of every citizen that allows them to select the best person for the job. In many nations, the voting age is 18 years old. Citizens can vote for political parties, but they can also learn about the value of citizenship through voting. Many individuals believe that one vote will not make a difference. It does. People can pick their representative by voting. It also allows the person the right to query and clarify the concerns. Everyone, regardless of gender, class, or employment, is guaranteed the right to vote. This is a picture of congruity and homogeneity [1]. While skipping the vote may appear to be harmless, the long-term repercussions are severe. The present voting method is based on electronic voting. Each voter will be allocated to a polling station based on the address shown on his or her National Identification Card (NIC), which is a one-of-a-kind number used to identify each person [2-5]. The right to vote is determined by a person's nationality, age, and criminal history. On election day, voters report to their allocated polling location, sign in front of a judge who validates their identification, place a watermark on their nails, select a candidate, and press the ballot button to cast their vote. The votes are tallied and the results are announced at the end of the election. This paper describes a safe online voting system that protects against a variety of security threats [6-11].

2. Types of Attacks

2.1. Ransomware

It's a hostile attack in which attackers encrypt data based on the demand payment to recover access. When an online voting system is attacked, the data hosted on the election servers may become unavailable, forcing the election to be halted. In some situations, the attackers may even make the information public.

2.2. Malware

Malware is a firmware that is designed to carry out an unauthorized process that compromises a system's confidentiality, integrity, or availability. In this sense, malware that tries to influence the contents of a vote or read the choices made by a voter might make online voting systems vulnerable.

2.3. Phishing

It tries to obtain sensitive information like credit card details and passwords through social engineering and trickery in e-mails.

3. Types of Voting Systems

3.1. Paper-Based Voting System

It is the conventional voting method that has been employed in many countries in the past. The results will be published using the punch card or tallied on paper. It is also known as manual voting collection. The voter may use a device to cast their vote in specific circumstances, but the votes are not stored anywhere in any mode of storage i.e database. Voting technologies in this category include paper polls, lever voting machines, mark-sense ballots, and many other procedures such as voting by mail. The paper ballot has developed over time and remains popular now. Candidates' names are mentioned on the paper polls and select their vote with the help of a writing tool. Election workers hand count the paper votes that are gathered in ballot boxes. The counting of cast votes in the voting process is time-consuming and prone to human error.

3.2. Lever Voting Machines

In 1892, the first lever voting machines were introduced in New York, New York. They are made up of a four-sided array of devices that may be configured as the name of the party and candidates on either side of the lever, or vice versa. The levers return to their original places when a voter exits the private chamber, the votes will be counted according to the rotation of the wheel linked. The counters display the number of votes cast on each lever after the voting procedure. There is no need for a paper ballot since the lever machines just sum up the votes as they are cast, eliminating the necessity for a recount. The Internet Policy Institute (IPI) states that this voting method prohibits people from voting for more than one candidate and that certain versions give an audit trail [9]. This process is still used in many countries, but lever machines are no longer produced.

3.3. Direct Recording Electronic Voting System (DRE)

This voting technique is built on electrical apparatus that electronically records and processes votes using microprocessor technology. It's the first voting method to use touch screens, pushbuttons, or a keyboard at the such as in a specialized way where the voters can cast their votes using the device of their own choice in the place of voting at the front end of the electoral process. The voting devices are linked to a stand-alone Personal Computer (PC) that records and tallies the votes in a digital format. It has the benefit that more than one voter can use the input device at the same time to register their vote, and all votes are counted on a single computer. There is no need for a paper poll in this voting system: after proof of vote is printed and placed on a ballot, the voter has passed in the voting place and confirmed his or her vote, which is logged in the storage of the device, the votes are recounted once again electronically.

3.4. Poll-site Electronic Ballot Voting

This technique is a type of vote casting the act of casting a ballot at a civic location. Election authorities supervise the whole process, from voter authentication through storage, transmission, or actual transportation of the totaled votes to the central office. It concerns election authorities' control over ICT systems. The voting options are shown on a display of the computer or a poll attached to the device, and people who vote can pick their choices by clicking on the screen, typing, or pressing the button. The votes are tabulated after the voting session and saved in databases. These systems can be connected to the central processing center via virtual private networks (VPNs) for the tabulation of all results.

3.5. Remote Voting System

This technique is the lower level of the Direct Recording Electronic Voting System. In that votes are broadcast over the communal Internet via a common network. In this approach, voters are electronically registered, recorded, and counted from a variety of private and public places, including homes, schools, workplaces, public libraries, and shopping precincts. The outputs are tallied and tabulated in the tabulation center, not at the polling. It is an excellent voting method since it allows customers to vote using more general technologies such as communicating via television, dialing the phone, messages, the Internet, etc.

3.6. Internet Voting

The usage of this technique is to cast a vote in a remote place such as a residence, work, school, or anywhere else where the voting client is controlled by the people who vote or a mediator. This is an optimal method of voting since it provides voters with the greatest amount of options in casting their ballots. Because of the concerns about data privacy and data authentication being communicated vs the voting suppleness, online voting has received a lot of attention.

4. Existing System

The asymmetric key cryptosystem is used in several existing protocols, including the Two Agency Protocol, Blind Signature, and Sensus protocols. Asymmetric key cryptography is significantly slower and more complicated than symmetric key cryptography [12-18]. Furthermore, these protocols are more complicated to establish, and the ordinary user will have a tough time following them correctly. It is advised to combine the effectiveness of a symmetric-key cryptosystem with the ease of a public-key cryptosystem (also called a hybrid cryptosystem). As a result, the current study was conducted to develop an alternative high-speed, fool-proof, and error-free electronic voting system.

5. Proposed System

A new voting mechanism based on a hybrid cryptosystem has been suggested and built. In Fig.1, the ballot is encrypted with the suggested symmetric key technique outlined above, and the secret key information is encrypted with Tallier's public key.

The Tallier then decrypts the digital envelope with his private key to obtain the secret key, and only the cast vote is decrypted with the secret key acquired. After that, a confirmation message will be sent to the Validator, who will set the voter's status bit. In the same transaction, the count for the associated candidate is updated.

It is clear from the simulation results that the future symmetric key method beats the existing approaches. The processing time is quite short.

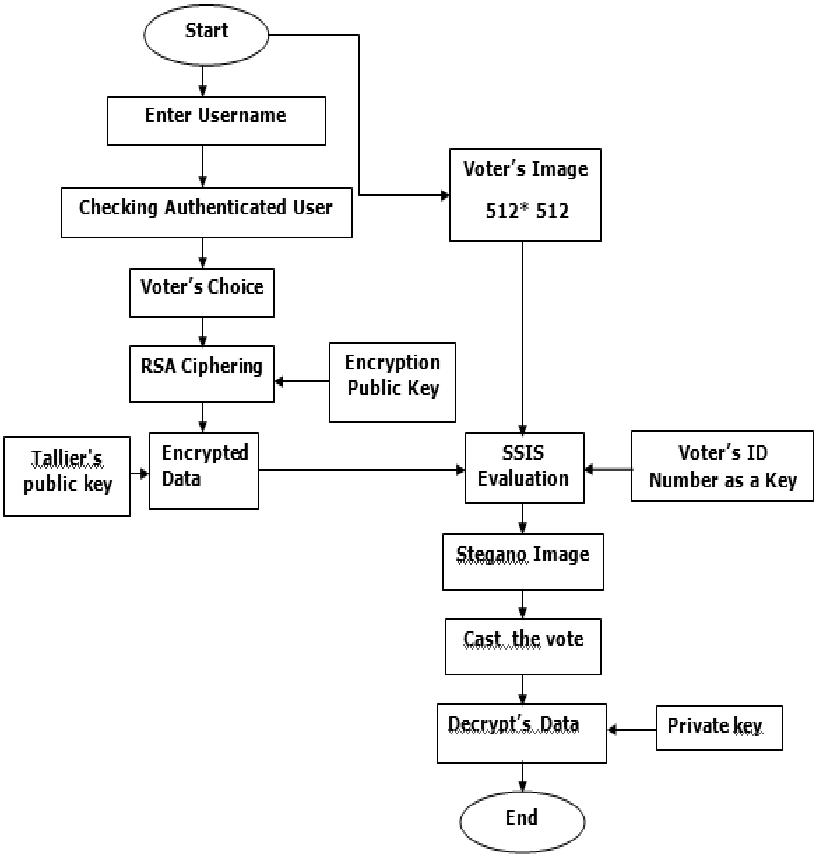

Fig.1. Use Case Diagram

6. Conclusion

Every democratic country relies heavily on voting. If this idea is adopted, the voting percentage will increase even further, as a small percentage of our countrymen work throughout the world and are unable to vote in their home nation. The online voting option is also available to persons who are physically impaired or extremely old. Because the Visual Cryptography Technique is utilized, the user can readily determine if he is on a phishing or legitimate site. The suggested internet voting system is quite successful, and it will assist the people who vote and organizations in several ways while also saving money and time.

Declarations

Source of Funding

This research work did not receive any grant from funding agencies in the public or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional and personal interests.

Consent for publication

Authors declare that they consented for the publication of this research work.

Authors' Contributions

All authors equally contributed in analysis and paper drafting.

References

[1] S. S. Rane, K. Adwait Phansalkar, M. Y. Shinde and A. Kazi, (2020). Avoiding Phishing Attack on Online Voting System Using Visual Cryptography. 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-4, doi: 10.1109/ICCCI48352.2020.9104071.

[2] S. Sridharan, (2013). Implementation of authenticated and secure online voting system. 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-7, doi: 10.1109/ICCCNT.2013.6726801.

[3] B. M. Pawar, S. H. Patode, Y. R. Potbhare and N. A. Mohota, (2020). An Efficient and Secure Students Online Voting Application. 2020 Fourth International Conference on Inventive Systems and Control (ICISC), pp. 1-4, doi: 10.1109/ICISC47916.2020.9171063.

[4] Krimmer, R., Triessnig, S., Volkamer, M. (2007). The Development of Remote E-Voting Around the World: A Review of Roads and Directions. In: Alkassar, A., Volkamer, M. (eds) E-Voting and Identity. Vote-ID 2007. Lecture Notes in Computer Science, vol 4896. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77493-8_1.

[5] Sroa, Rohit and Sinha, Priyanshu and Sharma, Ritwik and Rustagi, Parth and Sharma, Moolchand, (2021). A Visionary Approach to Smart Voting System (July 12, 2021). Proceedings of the International Conference on Innovative Computing & Communication (ICICC), Available at SSRN: https://ssrn.com/abstract=3884959 or http://dx.doi.org/10.2139/ssrn.3884959.

[6] S. P. Meduri, S. Kamatham, S. Subramanian, A. Meduri and N. Diwan, (2021). A Secure Network Monitored Balloting System. 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 31-35, doi: 10.1109/ICICT50816.2021.9358551.

[7] Thamaraimanalan, T., Jayaprada, D., Dhavasree, S., Kasthuri, K., & Deenathayalini, M. (2017). Aadhar Based Electronic Voting Machine. Asian Journal of Applied Science and Technology, 1(2): 145-147.

[8] Varsha Poddar, Sayan Mondal, Neelava Dutta, Hrishab Dey, (2018). Incorporating Advancements in Voting Strategies: A Survey. Ubiquitous Computing Electronics & Mobile Communication Conference (UEMCON) 9th IEEE Annual, pp. 249-254.

[9] Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, (2021). Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition. Computing Methodologies and Communication (ICCMC) 2021 5th International Conference, pp. 1471-1476.

[10] Loganathan T., Kamalkishore S., Navaneeth N., Krishnasamy N., Thamaraimanalan T (2017). Bus Tracking System. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(2): 399-401.

[11] Abdalla Al-Ameen and Samani Talab, (2013). The Technical Feasibility and Security of E-Voting. The International Arab Journal of Information Technology, 10(4): 397-404.

[12] H. Agarwal and G. N. Pandey, (2013). Online voting system for India based on AADHAAR ID. 2013 Eleventh International Conference on ICT and Knowledge Engineering, pp. 1-4, doi: 10.1109/ICTKE.2013.6756265.

[13] Thamaraimanalan, T., Naveena, D., Ramya, M., & Madhubala, M. (2020). Prediction and Classification of Fouls in Soccer Game using Deep Learning. Irish Interdisciplinary Journal of Science & Research, 4(3): 66-78.

[14] Z. A. Usmani, K. Patanwala, M. Panigrahi and A. Nair, (2017). Multi-purpose platform independent online voting system. 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-5, doi: 10.1109/ICIIECS.2017.8276077.

[15] S. Sridharan, (2013). Implementation of authenticated and secure online voting system. Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-7, doi: 10.1109/ ICCCNT.2013.6726801.

[16] Thamaraimanalan, T., RA, L., & RM, K. (2021). Multi biometric authentication using SVM and ANN classifiers. Irish Interdisciplinary Journal of Science & Research, 5(1): 118-130.

[17] J. Mutebi, E. Bagarukayo, I. Ssempebwa and M. Kalanda, (2018). Online Voting System with Reliable Voter Authentication Protocols. IST-Africa Week Conference (IST-Africa), pp. 1-9.

[18] H. Hussien and H. Aboelnaga, (2013). Design of a secured e-voting system. International Conference on Computer Applications Technology (ICCAT), pp. 1-5, doi: 10.1109/ICCAT.2013.6521985.